PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-321783
(43)Date of publication of application : 08.12.1995

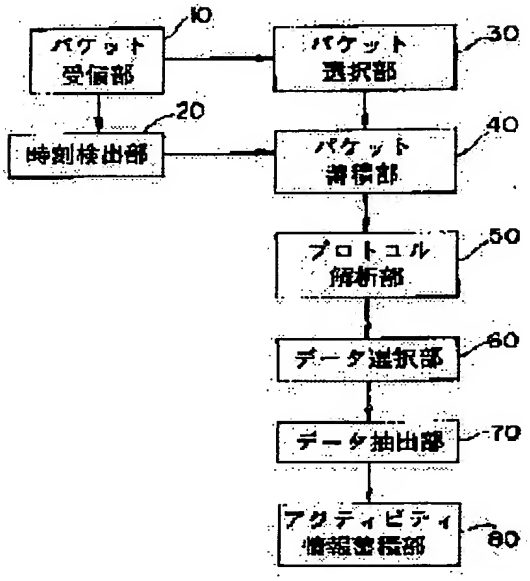
(51)Int.Cl. H04L 12/24
H04L 12/26
G06F 13/00
H04L 29/14
// G06F 15/16

(21)Application number : 06-111515
(22)Date of filing : 25.05.1994

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : YOKOYAMA MINEAKI

(54) NETWORK MONITOR EQUIPMENT

(57)Abstract:
PURPOSE: To provide a network monitor equipment in which the operating state of network application programs is monitored without giving effect onto traffic of the network and equipments making data communication.
CONSTITUTION: A packet selection section 30 selects a desired packet among packets received by a packet reception section 10 and stored the packet to a packet storage section 40. A protocol analysis section 50 analyzes the header of a data frame in the packet stored in the packet storage section 40 and provides an output of the result of analysis and data of an application layer after the header. A data selection section 60 estimates a data form and selects the data of the application layer based on the estimated data form and gives the data to a data extract section 70. The data extract section 70 extracts data required for monitoring from the received data and stores the data to an activity storage section 80.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平7－321783

(43)公開日　平成７年(1995)12月８日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/24					
	12/26					
Ｇ０６Ｆ	13/00	３５５	0832－5E			
			9466－5K	Ｈ０４Ｌ	11/ 08	
			9371－5K		13/ 00	３１３

審査請求　未請求　請求項の数１　ＯＬ　（全 ６ 頁）　最終頁に続く

(21)出願番号　特願平6－111515

(22)出願日　平成６年(1994) ５月25日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂三丁目３番５号

(72)発明者　横山　峰明
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ&Ｄ　ビジネスパークビル
富士ゼロックス株式会社内

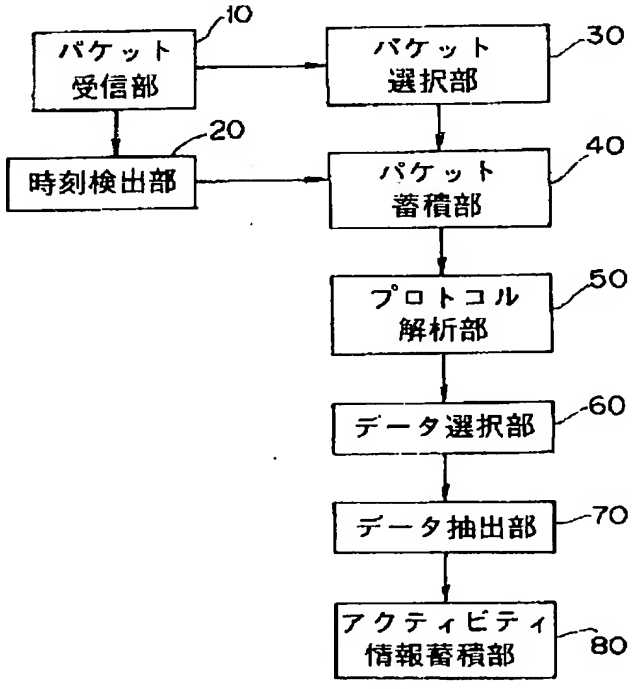
(74)代理人　弁理士　木村　高久

(54)【発明の名称】　ネットワーク監視装置

(57)【要約】

【目的】この発明は、ネットワークのトラフィック及びデータ通信する装置に影響を与えることなく、ネットワークアプリケーションの動作状況をモニタリングすることのできるネットワーク監視装置を提供する。

【構成】パケット選択部３０はパケット受信部１０によって受信されたパケットのうち、所望のパケットを選択し、パケット蓄積部４０に蓄積する。プロトコル解析部５０は、パケット蓄積部４０に蓄積されているパケット内のデータフレームのヘッダを解析し、該解析結果と当該ヘッダ以降のアプリケーション層のデータとを出力する。データ選択部６０は、データ形式を推定しこの推定されたデータ形式に基づいて前記アプリケーション層のデータを選択し、これをデータ抽出部７０に渡す。データ抽出部７０は、受け取ったデータから、モニタリングに必要なデータを抽出してアクティビティ蓄積部８０に蓄積する。



1

【特許請求の範囲】

【請求項１】　ネットワークに接続され、該ネットワークに伝送されるデータフレームを受信して解析するネットワーク監視装置において、

前記データフレームのうち、所望のデータフレームを選択する第１の選択処理処理手段と、

前記第１の選択処理手段の選択結果を記憶する第１の記憶手段と、

前記第１の記憶手段に記憶されたデータフレームのヘッダを解析し、該解析結果と当該ヘッダ以降のアプリケーション層のデータとを出力するプロトコル解析手段と、

前記プロトコル解析手段により得られたアプリケーション層のデータのデータ形式を推定し、必要なデータ形式のデータを選択する第２の選択処理手段と、

前記第２の選択処理手段の選択結果及びこれに対応する前記解析結果のうち必要な情報を記憶する第２の記憶手段とを具備したことを特徴とするネットワーク監視装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明はネットワークに伝送されるデータフレームを受信して解析するネットワーク監視装置に関する。

【０００２】

【従来の技術】従来、ネットワークのモニタにおいては、ネットワーク上のパケット単位での統計の集計／表示、及びパケツト内容の解析／表示を行っている。

【０００３】また他のモニタとしては、特開平４－１３７９４４号公報に記載されたプロトコル解析装置がある。この解析装置では、コネクション型プロトコルで通信しているノード間でやりとりしているデータグラムをもとに、各ノードにおけるコネクションの状態を検出して、例えばマトリクス型または時系列的に表示するようにしている。

【０００４】一方、ネットワークを利用するアプリケーションのアクディビティをモニタする方法としては、監視されるステーション側にエージェントと呼ばれるプログラムを実装し、そのエージェントに対して、問い合わせを行ったり、イベントを報告させることにより情報を得るのが一般的な方法である。

【０００５】

【発明が解決しようとする課題】しかしながら、上記公報のプロトコル解析装置を含めた上記従来のネットワークモニタでは、例えばプリントアウトの実行、ファイルへのアクセスなどのレベルでネットワークを利用するアプリケーションのアクティビティを解析し表示することはできなかった。

【０００６】なお、アプリケーションのアクティビティを解析し表示するには、処理の要求元と要求先の双方の状態をシミュレートし、その状態に基づきデータを解釈

2

する必要があり、複雑な処理が必要であった。

【０００７】また、上述したアプリケーションのアクディビティをモニタする方法すなわちエージェントを用いる方法にあっては、各ステーションにエージェントを組み込む必要があるため、モニタリングを前提としたネットワークシステムを構築する必要がある。このことは、エージェントを用いていない既存のネットワークシステムにおいては、当然ながらエージェントを用いることによるモニタリングの結果を得ることはできないことを意味する。またモニタリングすることにより、問い合わせ結果やイベントの報告情報がネットワーク上に転送されることになるので、ネットワークのトラフィクあるいは監視されるステーションの活動に影響を及ぼす虞が極めて高い。

【０００８】本発明は、ネットワークのトラフィック及びデータ通信する装置に影響を与えることなく、ネットワークアプリケーションの動作状況をモニタリングすることのできるネットワーク監視装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明は、ネットワークに接続され、該ネットワークに伝送されるデータフレームを受信して解析するネットワーク監視装置において、前記データフレームのうち、所望のデータフレームを選択する第１の選択処理処理手段（図１の３０）と、該第１の選択処理手段の選択結果を記憶する第１の記憶手段（図１の４０）と、該第１の記憶手段に記憶されたデータフレームのヘッダを解析し、該解析結果と当該ヘッダ以降のアプリケーション層のデータとを出力するプロトコル解析手段（図１の５０）と、該プロトコル解析手段により得られたアプリケーション層のデータのデータ形式を推定し、必要なデータ形式のデータを選択する第２の選択処理手段（図１の６０）と、該第２の選択処理手段の選択結果及びこれに対応する前記解析結果のうち必要な情報を記憶する第２の記憶手段（図１の８０）とを具備している。

【００１０】

【作用】この発明では、第１の選択処理手段が、ネットワークに伝送されるデータフレームのうち、所望のデータフレームを選択して第１の記憶手段に記憶し、プロトコル解析手段が、第１の記憶手段に記憶されたデータフレームのヘッダを解析し、該解析結果と当該ヘッダ以降のアプリケーション層のデータとを出力し、第２の選択処理手段が、前記アプリケーション層のデータのデータ形式を推定し、必要なデータ形式の前記アプリケーション層のデータを選択し、そして第２の記憶手段は、第２の選択処理手段の選択結果及び、これに対応する前記解析結果のうち必要な情報を記憶するようにしているので、ネットワーク上でのデータの送受を行うことなく、また、アプリケーションの状態をシミュレートするため

の複雑な処理を行うことなく、ネットワークアプリケーションの動作状況をモニタリングすることができる。

【００１１】

【実施例】以下、本発明の実施例を添付図面を参照して説明する。

【００１２】図１は、本発明に係るネットワーク監視装置の一実施例を示す機能ブロック図である。

【００１３】同図において、パケット受信部１０は、ネットワークに接続され、該ネットワークに転送されている全てのパケット（すなわちデータフレーム）を受信すると共に、この受信時刻を受信したパケットに付加し、更にそのパケッを時刻検出部２０及びパケット選択部３０に渡す。時刻検出部２０は、パケット受信部１０からのパケットの中から受信時刻を検出する。パケット選択部３０は、渡されたパケット中の特定位置のデータに基づいてパケットを選択する。パケット蓄積部４０には、パケット選択部３０によって選択されたパケットを時刻検出部２０からの受信時刻のデータと共に蓄積する。

【００１４】プロトコル解析部５０は、パケット蓄積部４０に蓄積されているパケットに含まれているプロトコルのヘッダを解析し、必要なプロトコル情報と、そのパケットにより送られるアプリケーションデータを抽出し、これらのデータをデータ選択部６０に渡す。

【００１５】なお、上記必要なプロトコル情報とは、例えば宛先及び発信元のアドレスなどであり、また上記アプリケーションデータとは、例えばＴＣＰ（トランスミッション・コントロール・プロトコル）より上位のデータ、即ち、セッション層からアプリケーション層までのデータのことである。

【００１６】データ選択部６０は、渡されたアプリケーションデータを解析して、該データのデータ形式を推定し、推定されたデータ形式に基づき該データがモニタリングに必要なデータであるか否かを判定し、必要なデータのみを選択する。すなわち、アプリケーションに関する知識、及びそのモニタリングに必要なデータに関する固有の知識に基づき、渡されたアプリケーションデータのデータ形式を推定し、必要なデータか否かを判定する。ここで、データ選択部６０は、字句解析によりデータが特定の文法に従うか否かによって、データが所望のデータ形式のものか否かを推定し、所望のデータ形式であると推定されたアプリケーションデータのみを選択するようにしている。

【００１７】データ抽出部７０は、データ選択部６０により選択されたデータ、プロトコル解析の結果及び受信時刻データから必要なものを取り出す。

【００１８】アクティビティ情報蓄積部８０は、データ抽出部７０により抽出されたデータを蓄積する。

【００１９】次に、ＵＮＩＸシステムにおけるリモートプリントのモニタリングを行う場合の処理について説明する。

【００２０】ＵＮＩＸシステムにおけるリモートプリントは、lpdデーモン間のＴＣＰプロトコルによるデータ転送により行われる。転送されるデータは、プリントコントロールファイルとプリントデータファイルである。これらのファイルのデータは、コマンドバイトに続きファイルサイズ、ファイル名を含んだメッセージに続き送られる。この転送の手順を図２に示す。

【００２１】図２に示される例の転送されるデータの内容について説明する。

【００２２】［ ＼００２　ｐｒｉｎｔｅｒｎａｍｅ ＼０１２ ］について

“ ＼００２（８進数で２）”はこれに続く文字列がプリンタ名またはコントロールファイルとそのサイズであることを示すコマンドバイトを表している。この場合、“ｐｒｉｎｔｅｒｎａｍｅ”はプリンタ名を表す文字列がコマンドバイトに続くことを表している。“＼０１２（８進数０１２）”はコマンドの終わりを示す１バイトのデータである。これ全体で出力先プリンタがコマンドバイトに続く文字列で示されたものであることを意味している。

［ ＼０００ ］について

“＼０００ ”は応答を示すコマンドバイトである。これでコマンドの受理を意味している。

【００２３】［ ＼００３　ｓｉｚｅ　ｆｉｌｅｎａｍｅ ＼０１２ ］について

“＼００３”はこれに続く文字列が転送されるファイルのサイズとファイル名であることを示すコマンドバイトである。“ｓｉｚｅ”はコマンドバイトに続きファイルサイズを表す数字列が続くことを表し、“ｆｉｌｅｎａｍｅ” はそれに続き空白をはさんでファイル名を表す文字列が続くことを意味する。“＼０１２”は上記と同様である。

【００２４】［ ｄａｔａ＼０００ ］について

“ｄａｔａ”は実際のデータを表し、“＼０００”はデータの終わりを表している。

【００２５】［ ＼００２　ｓｉｚｅ　ｆｉｌｅｎａｍｅ ＼０１２ ］について

これは、上述した＼００２コマンドバイトにおいてコントロールファイル名とそのサイズが続く場合のものである。

【００２６】図２に示される様に、上述したlpd間のデータ転送は、printer（プリンター）ポートと呼ばれる事実上固定のポートに対して行われる。また、コマンドバイト及びそれに続くパラメータは１つのメッセージ単位として送られるので、コマンドバイトは１つのパケットで送られるデータの先頭に位置する。

【００２７】ここでは、リモートプリントのモニタとしては、一例として、転送の起こった時刻、データファイルのサイズ、リモートプリントを発行したステーション、リモートプリントを受けたステーションの項目につ

いてモニタリングするものとする。

【００２８】このような前提条件下において、モニタリングの処理について図３及び図４を参照して説明する。

【００２９】図３はパケットの受信処理及び選択処理の動作を示すフローチャートであり、図４はモニタリングに必要なデータの抽出処理の動作を示すフローチャートである。

【００３０】最初にパケットの受信処理及び選択処理について説明する。

【００３１】図３において、パケット受信部１０は、モニタリングが終了したか否かを判断し（ステップ１１０）、終了していない場合は１パケットを受信すると共に（ステップ１２０）、このパケットをパケット選択部３０に渡す。これと並行して、時刻検出部２０はパケット受信部１０が受信したパケットの受信時刻を検出する（ステップ１３０）。

【００３２】パケット選択部３０は、パケット受信部１０から渡されたパケットは、ＴＣＰプロトコルのフォーマットに基づいているか否かに応じてＴＣＰパケットか否かを判断する（ステップ１４０）。ここで、ＴＣＰパケットの場合はパケット受信部１０から渡されたパケット中の特定位置のデータすなわちポート番号に基づいてprinterポート宛パケットか否かを判断する（ステップ１５０）。

【００３３】ここで、printerポート宛パケットの場合、パケット選択部３０は、そのパケットデータをパケット蓄積部４０に蓄積する。これと同時に、そのパケットの受信時刻データについても、時刻検出部２０によってパケット蓄積部４０に蓄積される（ステップ１６０）。

【００３４】このステップ１６０が終了した後は、上記ステップ１１０に戻り、このステップ以降が実行される。

【００３５】また上記ステップ１４０及びステップ１５０において「NO」の場合は、上記ステップ１１０に戻る。このステップ１１０においてモニタリングが終了した場合は処理を終了する。

【００３６】次にモニタリングに必要なデータの抽出処理について説明する。

【００３７】図４ににおいて、プロトコル解析部５０は、モニタリングが終了したか否かを判断し（ステップ２１０）、終了している場合には処理を終了し、一方、終了していない場合は、パケット蓄積部４０から、１パケット分のパケットデータを取り出す（ステップ２２０）。またプロトコル解析部５０は、取り出したパケットデータ内のＬＬＣ（論理リンク制御），ＩＰ（インターネットプロトコル）及びＴＣＰ（トランスミッションプロトコル）プロトコルヘッダの解析を行うと共に（ステップ２３０）、ソース及びデスティネーションのＩＰアドレス、及びＴＣＰプロトコル上のデータ（つまりアプリケーションデータ）を抽出し、これらの抽出結果をデータ選択部６０に渡す。この時、当該パケットの受信時刻データも渡される。

【００３８】データ選択部６０では、渡された抽出結果のうちアプリケーションデータについて字句解析を行い（ステップ２４０）、当該データが、値＼００３のバイト、数字列、空白及びＵＮＩＸファイル名の規則に従った文字列及び改行コードバイトにより構成されるものであるか否かを判断する（ステップ２５０）。

【００３９】ここで、該当するデータの場合は、データ選択部６０は、当該データ（アプリケーションデータ）と、既にプロトコル解析部５０から受け取っているソース及びデスティネーションのＩＰアドレス、及び受信時刻データとをデータ抽出部７０に渡す。

【００４０】データ抽出部７０は、数字列として、データ選択部６０から渡された上記データ中に含まれるファイルサイズデータを取り出すとともに（ステップ２６０）、このファイルサイズデータと、既にデータ選択部６０から受け取っている受信信時刻データ、ソース及びデスティネーションのＩＰアドレスデータをアクティビティ情報蓄部８０に蓄積する（ステップ２７０）。

【００４１】このステップ２７０を終了した後は、上記ステップ２１０に戻り、このステップ以降が実行される。また上記ステップ２５０において「NO」の場合は、上記ステップ２１０に戻る。

【００４２】以上説明したように本実施例によれば、通常のパケットのフィルタリングに加え、特定のアプリケーションに関す知識、及びモニタリングに必要な情報に関する知識に基づき、効率よくネットワークアプリケーションのモニタリングに必要なデータを収集することができる。

【００４３】このため、アプリケーションレベルでのアクティビティのモニタリングが可能となる。

【００４４】また、必要なデータのみを蓄積するのでデータ蓄積のための領域を削減することができる。

【００４５】さらに、パケット単位での解析が可能であり、ＩＰにおけるセグメンテーション分割、コネクション型のプロトコルにおけるコネクション管理など複雑なメカニズムを必要としない。

【００４６】

【発明の効果】以上詳細に説明したように本発明によれば、第１の選択処理手段が、ネットワークに伝送されるデータフレームのうち、所望のデータフレームを選択して第１の記憶手段に記憶し、プロトコル解析手段が、第１の記憶手段に記憶されたデータフレームのヘッダを解析し、該解析結果と当該ヘッダ以降のアプリケーション層のデータとを出力し、第２の選択処理手段が、プロトコル解析手段により得られたアプリケーション層のデータのデータ形式を推定し、必要なデータ形式のデータを選択し、そして第２の記憶手段は、第２の選択処理手段

の選択結果及び、これに対応する前記解析結果のうち必要な情報を記憶するようにしているので、ネットワークのトラフィック及びデータ通信する装置に影響を与えることなく、ネットワークアプリケーションの動作状況をモニタリングすることができる。

【００４７】従って、エージェントが組み込まれていない既存のネットワークシステムにおいても、ネットワークアプリケーションの動作状況をモニタリングすることができる。

【図面の簡単な説明】

【図１】本発明に係るネットワーク監視装置の一実施例＊

＊を示した機能ブロック図。

【図２】本実施例のモニタリングを説明するたもの図。

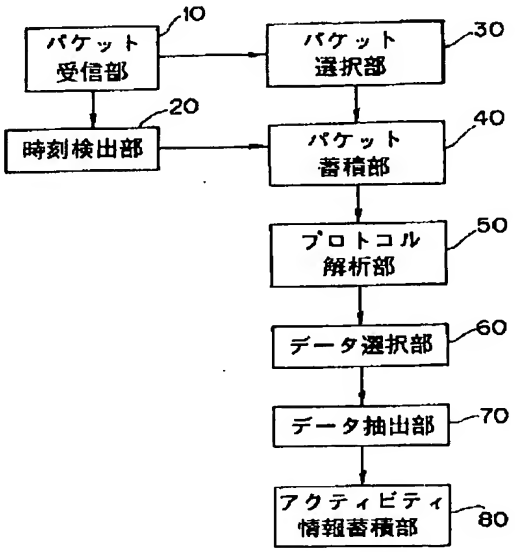
【図３】本実施例におけるパケットの受信処理及び選択処理の動作を示すフローチャート。

【図４】本実施例におけるモニタリングに必要なデータの抽出処理の動作を示すフローチャート。

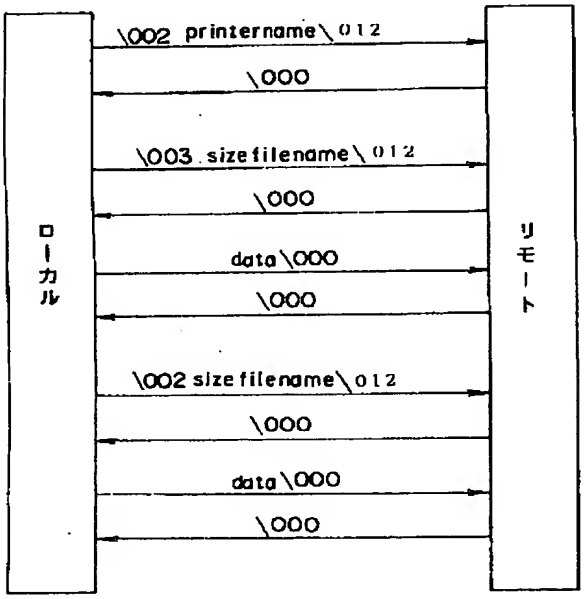
【符号の説明】

１０…パケット受信部、２０…時刻検出部、３０…パケット選択部、４０…パケット蓄積部、５０…プロトコル解析部、６０…データ選択部、７０…データ抽出部、８０…アクティビティ情報蓄積部。

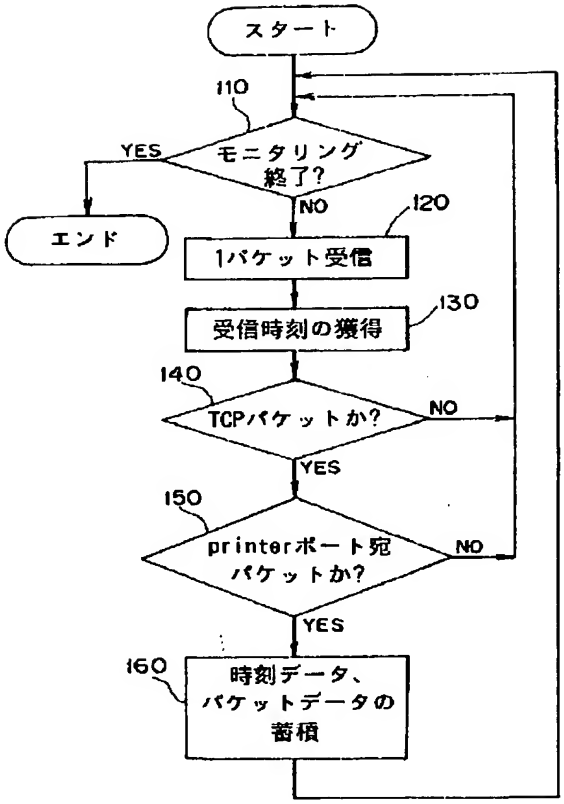
【図１】



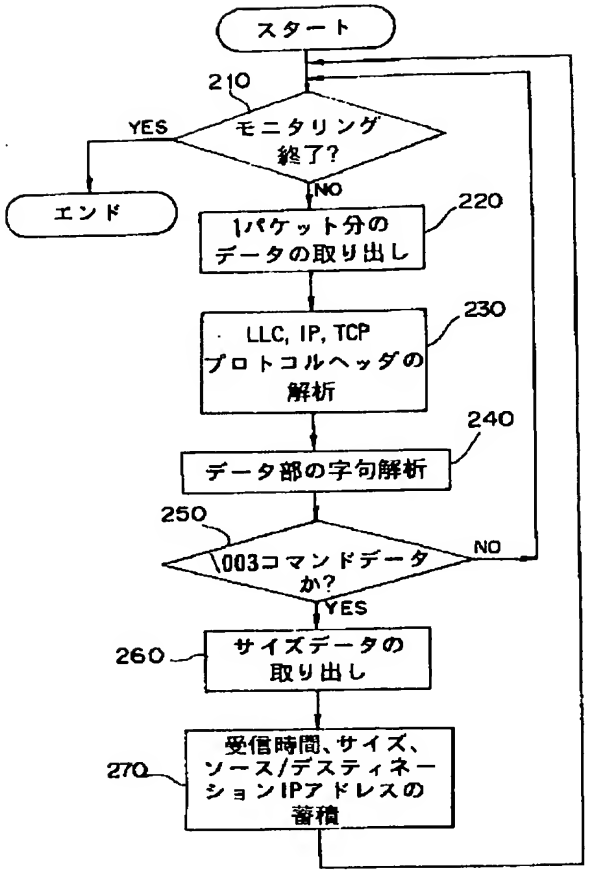
【図２】



【図３】



【図４】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　29/14				
// Ｇ０６Ｆ　15/16		４５０　Ｄ		